CLAIMS

1. A method for rendering encrypted digital content on a first device having a public key (PU1) and a corresponding private key (PR1), the digital content being encrypted according to a content key (KD), the method comprising:

obtaining a digital license corresponding to the content, the digital license including the content key (KD) therein in an encrypted form;

decrypting the encrypted content key (KD) from the digital license to produce the content key (KD);

obtaining from the first device the public key thereof (PU1);

encrypting the content key (KD) according to the public key (PU1) of the first device (PU1 (KD)); and

composing a sub-license corresponding to and based on the obtained license, the sub-license including (PU1 (KD)), and transferring the composed sub-license to the first device, wherein the first device can decrypt (PU1 (KD)) with the private key thereof (PR1) to produce the content key (KD), and can render the encrypted content on the first device with the produced content key (KD).

2. The method of claim 1 further comprising, prior to composing the sub-license and transferring the composed sub-license to the device, checking the obtained license to determine that such license permits issuance of the sub-license to the device.

3. The method of claim 1 further comprising transferring the content to the first device.

4. The method of claim 1 for rendering encrypted digital content on a first device having a digital rights management (DRM) system, the DRM system having the public key (PU1) and the corresponding private key (PR1), the method comprising:

obtaining from the first device the public key of the DRM system thereof (PU1);

encrypting the content key (KD) according to the public key (PU1) of the DRM system of the first device (PU1 (KD)); and

composing a sub-license corresponding to and based on the obtained license, the sub-license including (PU1 (KD)), and transferring the composed sub-license to the first device, wherein the DRM system of the first device can decrypt (PU1 (KD)) with the private key thereof (PR1) to produce the content key (KD), and can render the encrypted content on the first device with the produced content key (KD).

5. The method of claim 1 comprising:

obtaining the digital license and storing the obtained digital license on a second device;

decrypting the encrypted content key (KD) from the digital license on the second device to produce the content key (KD);

obtaining from the first device the public key thereof (PU1);

encrypting the content key (KD) according to the public key (PU1) of the first device (PU1 (KD)); and

composing a sub-license corresponding to and based on the obtained license, the sub-license including (PU1 (KD)), and transferring the composed sub-license from the second device to the first device, wherein the first device can decrypt (PU1 (KD)) with the private key thereof (PR1) to produce the content key (KD), and can render the encrypted content on the first device with the produced content key (KD).

6. The method of claim 5 wherein the second device has a public key (PU2) and a corresponding private key (PR2), the method comprising:

obtaining a digital license corresponding to the content, the digital license including the content key (KD) encrypted according to the public key (PU2) of the second device (PU2 (KD)); and

decrypting (PU2(KD)) from the digital license according to the private key (PR2) of the second device to produce the content key (KD).

7. The method of claim 5 wherein the second device is a computer.

8. The method of claim 1 wherein, the first device is a portable device.

9. The method of claim 1 wherein obtaining from the first device the public key thereof (PU1) comprises receiving a certificate from the first device within which is (PU1).

10. The method of claim 9 further comprising comparing the received certificate against a revocation list to ensure that the certificate has not been compromised.

11. The method of claim 9 comprising receiving a certificate from the first device within which is (PU1) and information relating to the first device.

12. The method of claim 11 further comprising, prior to composing the sub-license and transferring the composed sub-license to the device, checking the obtained license to determine that such license permits issuance of the sub-license to the device, such checking including employing the

information relating to the first device to determine whether the license permits issuance of the sub-license.

13. The method of claim 11 comprising receiving a certificate from the first device within which is (PU1) and information relating to at least one of the name, type, and manufacturer of the first device.

14. The method of claim 1 further comprising obtaining (PU1 (KD)) from the transferred sub-license, applying (PR1) to (PU1 (KD)) to obtain the content key (KD), and applying (KD) to decrypt the encrypted content, all by the first device.

15. A method for rendering encrypted digital content on a first device having a public key (PU1) and a corresponding private key (PR1), the digital content being encrypted according to a content key (KD), the method comprising:

providing the public key (PU1) to a second device, wherein the second device obtains a digital license corresponding to the content, the digital license including the content key (KD) therein in an encrypted form, decrypts the encrypted content key (KD) from the digital license to produce the content key (KD), encrypts the content key (KD) according to the public key (PU1) of the first device (PU1 (KD)), and composes a sub-license corresponding to and based on the obtained license, the sub-license including (PU1 (KD));

receiving the composed sub-license from the second device;

obtaining (PU1 (KD)) from the received sub-license;

applying (PR1) to (PU1 (KD)) to obtain the content key (KD);

applying (KD) to decrypt the encrypted content; and

rendering the decrypted content.

16. The method of claim 15 further comprising receiving the content from the second device.

17. The method of claim 15 for rendering encrypted digital content on a first device having a digital rights management (DRM) system, the DRM system having the public key (PU1) and the corresponding private key (PR1), the digital content being encrypted according to a content key (KD), the method comprising:

providing the public key (PU1) of the DRM system to the second device;

receiving the composed sub-license from the second device;

obtaining (PU1 (KD)) from the received sub-license;

applying the private key (PR1) of the DRM system to (PU1 (KD)) to obtain the content key (KD);

applying (KD) to decrypt the encrypted content; and

rendering the decrypted content.

18. The method of claim 15 wherein the second device is a computer.

19. The method of claim 15 wherein, the first device is a portable device.

20. The method of claim 15 wherein providing the public key (PU1) to the second device comprises providing a certificate to the second device within which is (PU1).

21. The method of claim 20 wherein providing the public key (PU1) to the second device comprises providing a certificate to the second device

within which is (PU1) and information relating to the first device, wherein the second device can employ the information relating to the first device to determine whether the obtained license permits issuance of the sub-license.

22. The method of claim 21 comprising providing the certificate to the second device within which is (PU1) and information relating to at least one of the name, type, and manufacturer of the first device.

23. A method of checking out a sub-license to a first device from a second device comprising:

receiving a request from the second device for a nonce, and providing such nonce;

receiving from the second device the checked-out sub-license and the provided nonce;

concluding that the nonce received is the same nonce provided;

therefore concluding that the received sub-license is legitimate; and

storing the sent sub-license.

24. The method of claim 23 in combination with a method of checking in the checked-out sub-license comprising deleting the checked-out sub-license and then providing a trusted indication to the second device that the checked-out sub-license has in fact been deleted.

25. The method of claim 24 wherein the second device adds the checked-out sub-license to a catalog by adding an entry including an identifier identifying the checked-out sub-license and an identifier identifying the first device to the catalog, and wherein checking in the checked-out sub-license comprises:

requesting a nonce from the second device, and receiving such nonce; and

sending to the second device the received nonce, an identifier identifying the first device, and a list of all sub-licenses currently resident on the first device, wherein the deleted checked-out sub-license is not in the sent list, and wherein the second device concludes that the nonce sent by the first device is the same nonce received by the first device, therefore concludes that the sent identifier and list that accompanied the sent nonce is legitimate, compares the sent list with the catalog and notes that the deleted checked-out sub-license is in the catalog but not on the sent list, and deletes the entry having the identifier identifying the deleted checked-out sub-license and the identifier identifying the first device from the catalog.

26. A method of checking out a sub-license from a second device to a first device comprising:

requesting a nonce from the first device, and receiving such nonce; and

sending the checked-out sub-license and the received nonce to the first device, wherein the first device concludes that the nonce sent by the second device is the same nonce received by the second device, therefore concludes that the sent sub-license that accompanies the sent nonce is legitimate, and stores the sent sub-license.

27. The method of claim 26 further comprising adding the checked-out sub-license to a catalog.

28. The method of claim 27 wherein adding the checked-out sub-license to the catalog comprises adding an entry including an identifier identifying the checked-out sub-license and an identifier identifying the first device to the catalog.

29. The method of claim 27 in combination with a method of checking in the checked-out sub-license comprising receiving a trusted indication from the first device that the checked-out sub-license has been deleted.

30. The method of claim 29 wherein checking in the checked-out sub-license comprises:

receiving a request from the first device for a nonce, and providing such nonce;

receiving from the first device the provided nonce, an identifier identifying the first device, and a list of all sub-licenses currently resident on the first device, wherein the deleted checked-out sub-license is not in the sent list;

concluding that the received nonce is the same nonce provided;

therefore concluding that the received identifier and list is legitimate;

comparing the received list with the catalog, and noting that the deleted checked-out sub-license is in the catalog but not on the sent list; and

deleting the entry having the identifier identifying the deleted checked-out sub-license and the identifier identifying the first device from the catalog.

31. A method of checking out a sub-license from a second device to a first device comprising:

requesting, by the second device, a nonce from the first device, and receiving such nonce;

sending, by the second device, the checked-out sub-license and the received nonce to the first device;

concluding, by the first device, that the nonce sent by the second device is the same nonce received by the second device;

therefore concluding, by the first device, that the sent sub-license that accompanies the sent nonce is legitimate; and

storing, by the first device, the sent sub-license.

32. The method of claim 31 further comprising adding, by the second device, the checked-out sub-license to a catalog.

33. The method of claim 32 wherein adding the checked-out sub-license to the catalog comprises adding an entry including an identifier identifying the checked-out sub-license and an identifier identifying the first device to the catalog.

34. The method of claim 32 in combination with a method of checking in the checked-out sub-license comprising deleting the checked-out sub-license from the first device and then providing a trusted indication to the second device that the checked-out sub-license has in fact been deleted.

35. The method of claim 34 wherein checking in the checked-out sub-license comprises:

deleting, by the first device, the checked-out sub-license therefrom;

requesting, by the first device, a nonce from the second device, and receiving such nonce;

sending, by the first device to the second device, the received nonce, an identifier identifying the first device, and a list of all sub-licenses currently resident on the first device, wherein the deleted checked-out sub-license is not in the sent list;

concluding, by the second device, that the nonce sent by the first device is the same nonce received by the first device;

therefore concluding, by the second device, that the sent identifier and list that accompanied the sent nonce is legitimate;

comparing, by the second device, the sent list with the catalog, and noting that the deleted checked-out sub-license is in the catalog but not on the sent list; and

deleting, by the second device, the entry having the identifier identifying the deleted checked-out sub-license and the identifier identifying the first device from the catalog.